(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日:
2005年2月10日(10.02.2005)

PCT

(10) 国际公布号:
WO 2005/013558 A1

(51) 国际分类号[7]: H04L 12/26

(21) 国际申请号: PCT/CN2003/001069

(22) 国际申请日: 2003年12月16日(16.12.2003)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
03149767.5 2003年8月5日(05.08.2003) CN

(71) 申请人(对除美国以外的所有指定国): 中兴通讯股份有限公司(ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人;及
(75) 发明人/申请人(仅对美国): 乔克智(QIAO, Kezhi) [CN/CN]; 倪明(NI, Ming) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(74) 代理人: 北京市中咨律师事务所(ZHONGZI LAW OFFICE); 中国北京市西城区阜成门北大街6号-9国际投资大厦C座17层, Beijing 100034 (CN)。

(81) 指定国(国家): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

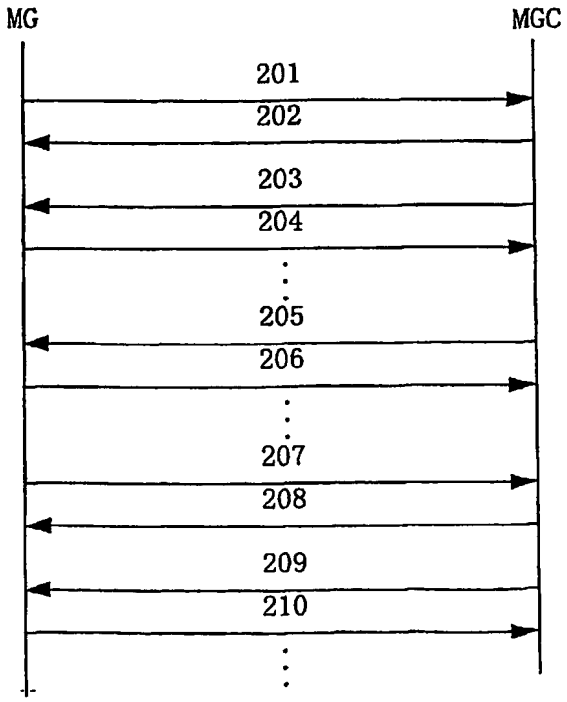
(84) 指定国(地区): ARIPO专利(BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚专利(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲专利(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI专利(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

本国际公布:
— 包括国际检索报告。

所引用双字母代码和其它缩写符号，请参考刊登在每期PCT公报期刊起始的"代码及缩写符号简要说明"。

(54) Title: AUTHENTICATION METHOD FOR MEDIC GATEWAY

(54) 发明名称: 媒体网关鉴权的方法



(57) Abstract: The present invention relates to an authentication method for Media Gateway, including the following step: Set up an initial key between the Media Gateway and Media Gateway Controller, for validate the both sides initial digital signature; performs signaling communication between the said Media Gateway and the said Media Gateway Controller by use of the said initial key, to generates a new shared key which have a special lifetime. The said Media Gateway and the said Media Gateway Controller authenticate the call and response using the said new shared key. If the lifetime of the said shared key is finished, then the said Media Gateway and the said Media Gateway Controller updates the said shared key. The invention authenticate each call, update the shared key periodic, prevent calling out illegally effectively.

[见续页]

WO 2005/013558 A1

(57) 摘要

本发明涉及媒体网关鉴权的方法，包括以下步骤：为媒体网关和媒体网关控制器之间设定一个用于验证双方初始数字签名的初始密钥；所述媒体网关和所述媒体网关控制器用所述初始密钥进行信令通信，以生成新的具有特定生存期的共享密钥；所述媒体网关和所述媒体网关控制器用所述新的共享密钥对呼叫和应答进行鉴权；若所述新的共享密钥的生存期结束，则所述媒体网关和所述媒体网关控制器更新所述共享密钥。本发明能对每个呼叫都进行鉴权，定期更换共享密钥，有效防止不合法呼叫。